AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) An arrangement for audio, video, and data communications across packet based networks implementing the H.323 standard recommended by the International Telecommunications Union, the arrangement including one ~~ore~~ or more gatekeepers ~~(3)~~, ~~characterised in~~

~~that~~ wherein end-user ~~(1)~~ authentication is performed by ~~means of~~ an authentication proxy ~~(2)~~.

2. (Currently Amended) An arrangement according to claim 1, ~~characterised in that~~wherein a security profile used by ~~an~~ the authentication proxy ~~(2)~~ is supported by a gatekeeper ~~(3)~~ associated with said authentication proxy ~~(2)~~.

3. (Currently Amended) An arrangement according to claim 1, ~~characterised in that~~wherein end-user information needed by ~~an~~ the authentication proxy ~~(2)~~ is requested from ~~the~~ an end-user ~~(1)~~ by ~~means of~~ a non-proprietary communications protocol.

4. (Currently Amended) An arrangement according to claim 1, ~~characterised in that an~~wherein the authentication proxy ~~(2)~~ communicates information to a gatekeeper ~~(2)~~ by ~~means of~~ a H.323 version 2 RAS (Registration, Admission and Signaling) message.

5. (Currently Amended) An arrangement according to claim 3, ~~characterised in that a~~wherein the non-proprietary communications protocol ~~is selected form a group of non-proprietary protocols comprising~~includes one of http and https.

6. (Currently Amended) An arrangement according to claim 1, ~~characterised in that~~wherein information for end-user ~~(1)~~ authentication is provided by ~~the~~ an end-user ~~(1) by means of~~in an html form, an applet, or a servlet.

PLEASE ADD NEW CLAIMS 7 - 22 AS FOLLOWS:

7. (New) An authentication proxy arrangement in a H.323 telecommunication network for allowing authentication of an end-user operating from an H.323 end-point without H.323v2 or H.235 authentication support and with a Gatekeeper requiring initial end-user authentication according to a first authentication protocol using H.235 and thus being unsupported by the end-point, the first authentication protocol being at least part of H.323v2 or a corresponding first security profile, said authentication proxy being adapted to form a signaling path for authentication of the end-point towards the Gatekeeper, the authentication proxy being arranged:

to obtain from the end-point of the end-user, by using a second protocol different from said first protocol, authentication data comprising an end-user password and an end-point network location specification,

to generate a first H.323 RAS (Registration, Admission and Signaling) message using said first protocol, said first H.323 RAS message presenting said obtained authentication data and including an authentication request requesting authentication of the end-user by the Gatekeeper on basis of said presented authentication data,

to transmit said first H.323 RAS message to the Gatekeeper,

to receive a second H.323 RAS message from the Gatekeeper in response to said first H.323 RAS message, to interpret said second H.323 RAS message from the Gatekeeper for detecting a confirmation or rejection of said authentication request, and

to generate and send to said end-point, on detection of said confirmation or rejection of said authentication request, an authentication confirm or reject message, respectively, using the second protocol.

8. (New) The arrangement of claim 7, wherein the end-point network location specification is an internet protocol (IP) address or a user name.

9. (New) The arrangement of claim 7, wherein obtaining the authentication data is performed by a simple html form, an applet, or a servlet.

10. (New) The arrangement of claim 9, wherein the applet is a signed applet.

11. (New) The arrangement of claim 7, wherein the second protocol includes http or https.

12. (New) The arrangement of claim 7, wherein said first H.323 RAS message is a H.323.V2 GRQ (Gatekeeper request) or a RRQ (Registration request), respectively including H.235 data that includes said authentication data.

13. (New) The arrangement of claim 12, wherein the second H.323 message is a GCF (Gatekeeper confirm) or a RCF (Registration confirm).

14. (New) The arrangement of claim 7, wherein the authentication proxy is arranged to sending to the end-point of the end-user an http-response indicating authentication failure if the second H.323 message is a GRJ (Gatekeeper reject).

15. (New) A method using an authentication proxy arrangement in a H.323 telecommunication network for allowing authentication of an end-user operating from an H.323 end-point (1) without H.323v2 or H.235 authentication support and intending to operate with a Gatekeeper requiring initial end-user authentication according to a first authentication protocol using H.235 and thus being unsupported by the end-point, the first authentication protocol being at least part of H.323v2 or a corresponding first security profile, said authentication proxy being adapted to form a signaling path for authentication of the end-point towards the Gatekeeper, said method including:

obtaining from the end-point of the end-user, by using a second protocol different from said first protocol, authentication data comprising an end-user password and an end-point network location specification,

generating a first H.323 RAS message using said first protocol, said first H.323 RAS message presenting said obtained authentication data and including an authentication request requesting authentication of the end-user by the Gatekeeper on basis of said presented authentication data,

transmitting said first H.323 RAS message to the Gatekeeper,

receiving a second H.323 RAS message from the Gatekeeper in response to said first H.323 RAS message,

interpreting said second H.323 RAS message from the Gatekeeper for detecting a confirmation or rejection of said authentication request, and

generating and sending to said end-point, on detection of said confirmation or rejection of said authentication request, an authentication confirm or reject message, respectively, using the second protocol.

16. (New) The method of claim 15, wherein the end-point network location specification is an internet protocol (IP) address or a user name.

17. (New) The method of claim 15, wherein obtaining the authentication data is performed by a simple html form, an applet, or a servlet.

18. (New) The method of claim 18, wherein the applet is a signed applet.

19. (New) The method of claim 15, wherein the second protocol includes http or https.

20. (New) The method of claim 15, wherein the first H.323 RAS message is a H.323.V2 GRQ (Gatekeeper request) or a H.323.V2 RRQ (Registration request), respectively, including H.235 data that includes said authentication data.

21. (New) The method of claim 15, wherein the second H.323 message is a GCF (Gatekeeper confirm) or a RCF (Registration confirm).

22. (New) The method of claim 15, including the step of sending to the end-point of the end-user an http-response indicating authentication failure if the second H.323 message is a GRJ (Gatekeeper reject).